

=====

AVERY DENNISON SOFTWARE VULNERABILITY NOTICE

AVERY DESIGNER 5.0 AND CDSTOMPER CLICK'N DESIGN 3D
MICROSOFT SECURITY BULLETIN MS06-026 / BLOODHOUND.EXPLOIT.74 VIRUS
JUNE 15, 2006

=====

**BLOODHOUND.EXPLOIT.74 VIRUS
VULNERABILITY: CRITICAL**

On June 13th, Symantec™ provided a Virus Definition Update that detects the Bloodhound.Exploit.74 virus. This virus affects a Windows Metafile (WMF) vulnerability that could allow remote code execution of the Windows Graphics Rendering Engine.

Windows Metafile (WMF) is a common graphic file format used in Microsoft Windows. It is an image format that can contain both vector and bitmap information. It is optimized for the Windows operating system.

The only image format reported as vulnerable to this exploit is the Windows Metafile.

This vulnerability could render a denial of service or potentially block login to your computer. The virus can be triggered thru infected e-mail attachments, or by viewing web pages or network shares (*shared drives*) containing the exploit.

No user interaction is required to trigger this virus.

AFFECTED SOFTWARE

According to Microsoft, affected software includes:

- Microsoft Windows 98
- Microsoft Windows 98 Second Edition (SE)
- Microsoft Windows Millennium Edition (ME)

As of June 15th, Microsoft has not identified any workarounds for this vulnerability on Windows 98, Windows 98 Second Edition (SE) or Windows Millennium Edition (ME).

According to Microsoft, the virus does not affect:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP Service Pack 2
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 Service Pack 1

Windows critical security updates for these platforms can be downloaded from the Windows Update Website at <http://go.microsoft.com/fwlink/?LinkID=21129>

AVERY SOFTWARE

Avery DesignPro 5.0 and CDStomper Click'N Design 3D have been scanned with Symantec™ June 13th virus definition and the virus was NOT detected in any Avery software.

Avery DesignPro 5.0 and CDStomper Click'N Design 3D include Windows Metafile (WMF) graphics in their clipart library. This vulnerability can affect these files once installed.

BASIC SECURITY BEST PRACTICES

Avery recommends that you:

- Keep your system and virus software up-to-date. Microsoft recommends using the latest Windows service pack. Use Virus detection software, and keep the definitions current.
- Do not open e-mail attachments from unknown sources.
- Scan all software downloaded from the Internet before running it on your computer.
- Use complex passwords in order to make it difficult to hack password files.
- Delete or quarantine infected files immediately.
- When viruses are detected on your office computer, report the incident immediately to your system administrator or information technology contact.